(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平7－68051

(43)公開日　平成７年(1995)３月14日

(51)Int.Cl.[6]	識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ａ６３Ｆ　9/22	Ｇ Ｈ			
Ｇ０４Ｆ　10/04		9008－2Ｆ		

審査請求　未請求　請求項の数６　ＦＤ　（全９頁）

(21)出願番号　特願平6－204521

(22)出願日　平成６年(1994)８月５日

(31)優先権主張番号　９３０９６７９

(32)優先日　1993年８月５日

(33)優先権主張国　フランス（ＦＲ）

(71)出願人　591032013
ジェムプリュス　カード　アンテルナショナル　ソシエテ　アノニム
GEMPLUS CARD INTERNATIONAL SOCIETE ANONYME
フランス国　13420　ジェムノ　パルク　ダクティヴィテ　ドゥ　ラ　プレーヌ　ドゥ　ジュク　アヴニュ　ドュ　ピック　ドゥベルターニュ（番地なし）

(72)発明者　パトリス　ペイレ
フランス国　シュマン　ドゥ　サン　フランソワ　ルクロ　ドュ　ポン（番地なし）

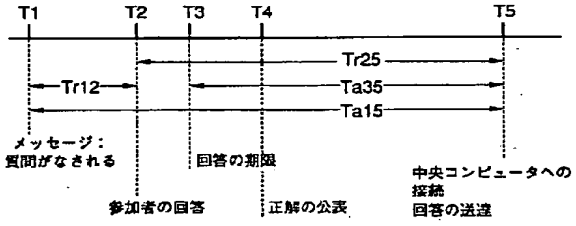
(74)代理人　弁理士　越場　隆

(54)【発明の名称】　イベントの時系列の検証を行う、対話式ゲームへの遠隔参加における安全システム

(57)【要約】

【構成】　安全保護されたマイクロプロセッサ（例えばマイクロ回路カード）を用いた連続する期間のカウントによって、イベントの時系列の検証を行う、対話式ゲームへの遠隔参加における安全システム。そのうち最初の期間（Ｔｒ１２）は、トランスミッタによって送信される暗号を用いて安全保護されたメッセージによって開始され、最後の期間（Ｔｒ２５）は、回答をトランスミッタの中央コンピュータに送るための、ゲーム機からトランスミッタの中央コンピュータへの接続によって終了される。

【作用】　テレビ放映される対話式ゲームに利用される。



1

【特許請求の範囲】

【請求項１】　テレビ番組の進行中にテレビ受像機によって受信される暗号メッセージを送信するトランスミッタ／中央コンピュータを備えた、対話式ゲームへの遠隔参加における安全システムであって、テレビ視聴者は、放映されたメッセージを読み取って、これらのメッセージ中になされる質問に対する回答を送り返すことの可能なゲーム機械を有し、該システムにおいては、

ゲーム機械が、連続する期間をカウントする手段を備え、このうち最初の期間（Ｔｒ１２）は、トランスミッタ／中央コンピュータによって送信されるメッセージによって開始され、最後の期間（Ｔｒ２５）は、ゲーム機械からトランスミッタ／中央コンピュータへの接続によって終了され、

最初の期間は、メッセージが受信される時間（ｔ１）とテレビ視聴者が回答する時間（ｔ２）によって規定され、最後の期間（Ｔｒ２５）は、テレビ視聴者が回答する時間（ｔ２）と回答がトランスミッタ／中央コンピュータへ送られる時間（ｔ５）によって規定され、

さらにゲーム機械は、回答を、上記のカウント結果と共に、トランスミッタ／中央コンピュータに送信するための手段を備え、

トランスミッタ／中央コンピュータが、

回答の期限（ｔ３）と回答が送られた時間（ｔ５）によって規定される期間（ｔａ３５）と、メッセージが送信された時間（ｔ１）と回答が送られてきた時間（ｔ５）によって規定される期間（ｔａ１５）をカウントする手段と、

Ｔｒ２５＞Ｔａ３５　および

Ｔｒ１２＋Ｔｒ２５＝Ｔａ１５±許容範囲の値

という関係のチェックを行い、さらにこの関係が検証されない場合には回答を拒絶するように構成されている計算およびチェック手段とを備えていることを特徴とする、対話式ゲームへの遠隔参加における安全システム。

【請求項２】　ゲーム機械のカウント手段が、クロックパルスカウントプログラムを実行する、クロックによって制御される安全保護されたマイクロプロセッサによって構成されていることを特徴とする請求項１に記載の対話式ゲームへの遠隔参加における安全システム。

【請求項３】　ゲーム機械のカウント手段が、クロックパルスカウントプログラムを実行する、内部クロックによって制御された計算手段によって構成されていることを特徴とする請求項１に記載の対話式ゲームへの遠隔参加における安全システム。

【請求項４】　放送番組に参加し、遠隔の中央コンピュータと協力して参加を認証するための機械であって、

中央コンピュータより送られてくるデジタル情報を受信するための手段と、

参加者によって、参加者の参加を表すデータ要素を導入されるためのインターフェース手段と、

2

中央コンピュータに接続を行うための手段と、

マイクロプロセッサとその記憶手段を備えた、少なくとも１つの安全保護された電子構成要素と、

少なくとも１つのクロック信号発生回路とをそなえ、

上記機械が、時間Ｔ１で、所定の形態を有するデジタルメッセージを受け取ると、そのメッセージを安全保護されたマイクロプロセッサに送り、

検証後に、安全保護されたマイクロプロセッサが、このメッセージをそのメモリに記録して、クロック信号発生回路によって与えられるクロック信号の期間に比例する時間ユニットのカウントを開始し、

時間Ｔ２で、機械が、この機械を所有するテレビ視聴者から、彼の参加に関するデータ要素を受け取ると、機械が、そのデータ要素を、安全保護されたマイクロプロセッサへと送信し、このマイクロプロセッサが、そのデータを、必要な形態でそのメモリ中に記録し、さらにこの瞬間の時間カウント値を記録し、

時間Ｔ５に、接続を行う手段によって、上記機械が中央コンピュータと接続されるまで、安全保護されたマイクロプロセッサがカウントを継続し、

接続が行われるとすぐに、マイクロプロセッサが、記憶されていた参加に関するデータ要素とカウント値Ｔｒ１２およびＴｒ２５を送信し、中央コンピュータが、これらの値がそれ自身のカウント値と一致することを検証し、さらに一致しない場合には回答を拒絶することを特徴とする、放送番組に参加するための機械。

【請求項５】　チップカード読み取り手段とチップカードを備え、上記チップカードが、マイクロプロセッサと作業メモリとプログラムメモリとを有する集積回路チップカードの形態の安全保護された構成要素を備えていることを特徴とする請求項４に記載の放送番組に参加するための機械。

【請求項６】　電子参加機械を有するテレビ視聴者の放送シナリオへの参加を管理する中央コンピュータ装置であって、

時間カウント手段と、

個々の電子参加機械にデジタルメッセージを放送する手段と、

個々の電子参加機械との接続を行うための手段と、

記憶処理手段とを備えており、

新規な放送シナリオが開始されると、時間Ｔ１に、この中央コンピュータ装置が適当な送信チャンネルを用いてデジタルメッセージをテレビ視聴者の個々の電子参加機械に放送して、さらに時間カウント手段を初期化して作動させ、

テレビ視聴者がそれ以上シナリオに参加できなくなる時間として選択された所定の時間Ｔ３に、時間カウント値を記憶して、このカウントを継続し、

電子参加機械が中央コンピュータに接続される時間として選択された時間Ｔ５に、電子参加機械によって得られ

た時間カウント値を記憶し、以下の関係をチェックする：

Ｔｒ２５＞Ｔａ３５で、

Ｔｒ１２＋Ｔｒ２５＝Ｔａ１５±許容範囲値

ここで：Ｔｒ２５はＴ２とＴ５の間の電子参加機械によるカウント期間であり、Ｔｒ１２はＴ１とＴ２の間の電子参加機械によるカウント期間であり、Ｔｒ３５はＴ３とＴ５の間の中央コンピュータによるカウント期間であり、Ｔｒ１５はＴ１とＴ５の間の中央コンピュータによるカウント期間であることを特徴とする装置。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、イベントの時系列の検証を行う、対話式ゲームへの遠隔または長距離参加における不正防止システムまたは安全システムに関するものである。

【０００２】

【従来の技術】いわゆる対話型テレビジョンシステムの出現によって、例えば、放送中に、局より放送された質問に対して視聴者が回答を行うように求められるような、視聴者のゲームへの参加を可能にすることが望まれている。そのようなゲームの最中に、テレビ視聴者が、ゲームの正解が局から示されてから回答したり、百科辞典やその他任意の参考データベースを参照してから回答したりするのを防ぐために、最大限の回答時間が設定されなければならない。さらに、サービスの供給者（ケーブルオペレータ、放送スタジオなど）が同時に送られてくる何千もの回答によって「飽和」するのを避けるために、テレビ視聴者の回答は即時に送られないようにするのが好ましい。そのためには、蓄積送信システムが必須である。このシステムでは、テレビ視聴者の回答は、その視聴者の家庭で、安全な方法で、大衆向け機器（例えばケーブルデコーダ、専用のゲーム機械など）に記憶され、後に、適当に時間をずらして、無線電話機、ケーブルその他任意の適当な電気通信手段によって送られる。

【０００３】そのようなシステムの例として、アメリカ合衆国で開発された、例えばインタラクティブゲームネットワークス（Interactive Game Networks)社により開発されたものがある。このシステムでは、テレビ視聴者は、ラジオインターフェースとキーボードとスクリーンとモデムとセキュリティモジュールとが設けられた小型のゲーム機械を持つ。そのようなシステムの操作を理解するために、イベントの時系列を示した図１を参照されたい。

【０００４】時間Ｔ１で、以下「中央コンピュータ」と称するトランスミッタ／中央コンピュータから質問が放送される。これらの質問は、ラジオによって上記のゲーム機械へと放送される。例えば、フットボールの試合の開始時に、テレビ視聴者は、前半の得点を予想するように求められる。この質問は、ゲーム機械のスクリーン上に現れる。時間Ｔ２に、参加している各テレビ視聴者により、ゲーム機械のキーボートを介して回答が入力され、ゲーム機械に装着されている安全チップ（スマートカードで使用されているタイプのもの）に記録される。質問が行われてから数分後、時間Ｔ３に、新しい放送信号が全てのゲーム機械をロックして、それ以上いかなる回答も受付けないようにする。その後、時間Ｔ４で、質問に対する解答が放送される（実際、この例では、Ｔ４はハーフタイムに相当する）。その後、時間Ｔ５に、記録された回答が、モデムにより、交換式電話ネットワークを通じてゲームの中央コンピュータへ送られ、参加の証明となる。テレビ視聴者が正解したならば、彼／彼女は何らかの賞金乃至賞品を受け取る。

【０００５】アメリカ合衆国特許第 4,592,546号に記載のような実施方法によれば、ゲーム機械内に設置された十分な精度を有するクロック回路を用いて、それぞれのイベントの日付け（時間）が記録される。参加者の回答がゲームの中央コンピュータに送られる時、ゲーム機械によって記録された時間も中央コンピュータに送られ、そのコンピュータによりその中に保存されていた基準時間と比較される。

【０００６】他に提案されている実施方法によれば、それぞれの大衆型ゲーム機械には、ゲームの中央コンピュータより送信される基準クロック信号と一定な間隔ごとに（例えば無線結合により）同期化される電子リアルタイムクロック回路が具備されている。質問が放送される時間Ｔ１と、回答がなされる時間Ｔ２は、ゲーム機械に記録される（例えば、安全保護された方法でスマートカード用のチップ内に記録される）。ゲーム中央コンピュータに接続が行われると、回答と記録された時間が、参加の証明として送られる。中央コンピュータは、送信時間Ｔ１に係わる情報が許容可能な範囲内であって、Ｔ２が、回答期限であるＴ３よりも前であることを確認する。

【０００７】

【発明が解決しようとする課題】上記のシステムにおいては、またはその他類似の実施態様においては、悪意を持ったユーザが、本人のゲーム機械に送られてくる制御信号（質問、ロッキング命令、クロック同期化信号など）を、適当な機械に記録する可能性がある。

【０００８】その場合、わずかに遅れた時点で、質問に対する解答が局より放送されるか、または特殊な捜索またはその他任意の手段によって彼の知るところとなったならば、この悪意を持った個人は、自分のゲーム機械の中で制御信号を繰り返し、リアルタイムの回答を装うことができる。これが可能となるのは、詐欺行為を行う個人には、自宅のプライバシーのなかで証人がおらず、さらにプレイ終了から次に期待される中央コンピュータへの回答の到達までの間には、常に十分に妥当な長さの時間が経過するためである。結局、ゲーム機械に、それが

外部から受信した信号（これは安全になされているはずのものである）が、本当に実時間に発生されたものであるか、またはそれらが、全く修正なしに記録された後でわずかな遅延を与えられているものかどうかを知るための手段をゲーム機械に備えるのは、経済的に不可能である。

【０００９】フランス特許出願第89 06848号として出願されてフランス特許出願公開公報第2 647- 619号として公開された特許、およびでフランス特許出願公開公報第2 658 357号として公開されたフランス追加特許第90 0 1512号には、プレイを遅らせることよって不正の防止を可能にするシステムが記載されている。そのシステムにおいては、中央コンピュータが、解答が放送された時間（または回答期限）Ｔ３と、テレビ視聴者による回答が中央コンピュータに送られた時間Ｔ５との間に経過する絶対時間をカウントし、時間Ｔ２において、テレビ視聴者の回答により、ゲーム機械内での現地時間カウント動作を起動させ、情報が中央コンピュータに送られる時間Ｔ５に、この中央コンピュータが、参加者宅のゲーム機械によって測定される時間Ｔ５－Ｔ２が、それ自身が計算した絶対時間Ｔ５－Ｔ３よりも間違いなく大であることを確認する。

【００１０】図２に示すタイミング図が、以上のシーケンスを示している。この特許で提案されている方法は、残念なことに絶対確実なものではない。なぜなら、ユーザは、現地時間カウンタを進めることによって、あたかも、回答と中央コンピュータへの接続との間に、実際に経過した時間よりも長い時間Ｔ５－Ｔ２が経過したかのように見せることができるからである。これは、ゲーム機械内に置かれた電子クロック回路の発振周波数を一時的に修正するだけで可能になる。

【００１１】実際、ゲーム機械内のカウンタは、それが物理的に保護されていない限りは、つまり樹脂内に埋め込まれていない限りは、ユーザにとってアクセス可能である。この回路がＲＣ発振器、セラミック共振器型発振器または水晶発振器のいずれによって供給されていても、その本来の周波数は、振動素子のわずかなミスマッチによって歪めることができる。従って、格別な困難を伴うことなく、発振周波数をわずかなパーセンテージ分だけ、高くしたり遅くすることが可能である。ゲーム機械のクロック回路に供給する発振器の発振周波数を高くすることによって、詐欺行為を行おうとする人は、期限Ｔ３が過ぎるまで待ち（例えば解答が生放送されるのを待ち）、その後ゲーム機械の発振器の発振周波数を高くして遅れを取り戻すことが可能である。従って、時間Ｔ５でこの個人のゲーム機械が中央コンピュータから問い合わせを受ける時には、この中央コンピュータに与えられる見掛けの時間Ｔ５－Ｔ２は、実際よりむしろ長くなる。

【００１２】マイクロ回路カードのある種のマイクロプロセッサに、クロック周波数の異常を検出するためのクロック周波数検出器を装備する方法が知られている。この種の検出器は、例えば、詐欺行為を行おうとする個人が、プロセッサによって実行されるプログラムに対して、“ステップバイステップ”法を試みるのを防ぐために、この構成要素に供給されるクロック周波数が極端に低い時に作動される。典型的には、このような低周波数検出器は、その構成要素の公称周波数が１MHz ～５MHzである時に、約500KHz未満で作動される。この種の検出器における精度の重大な欠落と、それが極端に低い周波数を検出するためだけに存在するという事実は、それが、上記のようなタイプの不正を防ぐためには使用できないことを意味する。

【００１３】本発明は、現在使用されているシステムの欠点を克服することを目的としたものである。実際、本発明の対象となるシステムは、テレビ視聴者が、間違いなく、質問が行われた時間とゲームの送信者によって決定された期限との間に質問に答えたという事実を確実に検証するために使用することができる。

【００１４】

【課題を解決するための手段】ここで提案されるシステムは、安全保護されたプロセッサ（例えばマイクロ回路カードプロセッサ）によって連続する時間間隔をカウントするという事に基づくもので、そのうち最初の間隔は、トランスミッタによって送信される暗号を用いて安全保護されたメッセージによって開始され、最後の間隔は、回答の証明を中央コンピュータに送るためにゲーム機械から中央コンピュータへの接続が行われることによって終了する。

【００１５】より詳細には、本発明によるならば、テレビ番組の進行中にテレビ受像機によって受信される暗号メッセージを送信するトランスミッタ／中央コンピュータを備えた、対話式ゲームへの遠隔参加における安全システムが提供される。テレビ視聴者は、放映されたメッセージを読み取って、これらのメッセージ中になされる質問に対する回答を送り返すことの可能なゲーム機械を有しており、該システムにおいては、ゲーム機械が、メッセージが受信される時間ｔ１とテレビ視聴者が回答する時間ｔ２によって規定される期間の長さＴｒ１２と、テレビ視聴者が回答する時間ｔ２と回答がトランスミッタ／中央コンピュータへ送られる時間ｔ５とで規定される期間の長さＴｒ２５をカウントする手段を備え、

【００１６】トランスミッタ／中央コンピュータが、回答の期限ｔ３と回答が送られた時間ｔ５によって規定される期間の長さｔａ３５と、メッセージが送信された時間ｔ１と回答が送られてきた時間ｔ５によって規定される期間の長さｔａ１５をカウントする手段を備え、さらに、Ｔｒ２５＞Ｔａ３５およびＴｒ１２＋Ｔｒ２５＝Ｔａ１５±許容範囲の値、という関係のチェックを行い、さらにこの関係が検証されない場合には回答を拒絶する

計算手段を備えている。ゲーム機械のカウント手段は、クロックパルスカウントプログラムを実行する、クロックによって制御された安全保護されたマイクロプロセッサによって構成されている。

【００１７】本発明によれば、さらに、放送番組に参加し、遠隔の中央コンピュータと協力して参加を認証するための機械は、中央コンピュータより送られてくるデジタル情報を受信する手段と、参加者によって、参加者の参加を表すデータ要素を導入するためのインターフェースと、中央コンピュータに接続を行うための手段と、マイクロプロセッサとその記憶手段を備えた、少なくとも１つの安全保護された電子構成要素と、少なくとも１つのクロック信号発生回路とを備え、

【００１８】機械が、時間Ｔ１で所定の形態を有するデジタルメッセージを受け取ると、そのメッセージを安全保護されたマイクロプロセッサに送り、検証後に、安全保護されたマイクロプロセッサがこのメッセージをそのメモリに記録して、クロック信号発生回路によって与えられるクロック信号の期間に比例する時間ユニットのカウントを開始し、時間Ｔ２で、機械が、この機械を所有するテレビ視聴者から、彼の参加に関するデータ要素を受け取ると、機械は、そのデータ要素を、安全保護されたマイクロプロセッサへと送信し、このマイクロプロセッサが、そのデータを、必要な形態でそのメモリ中に記録し、さらにこの瞬間の時間カウント値を記録し、

【００１９】時間Ｔ５で、接続を行う手段によってその機械が中央コンピュータと接続されるまで、安全保護されたマイクロプロセッサがカウントを継続し、接続が行われるとすぐに、マイクロプロセッサが、記憶されていた参加に関するデータ要素とカウント値Ｔｒ１２およびＴｒ２５を送信し、中央コンピュータが、これらの値がそれ自身のカウント値と一致することを検証し、さらに一致しない場合には回答を拒絶することができる。

【００２０】さらに、本発明によれば、電子参加機械を有するテレビ視聴者の放送シナリオへの参加を管理する中央コンピュータ装置は、時間カウント手段と、個々の電子参加機械にデジタルメッセージを放送する手段と、個々の電子参加機械との接続を行うための手段と、記憶処理手段とを備えており、

【００２１】放送シナリオが開始されると、時間Ｔ１に、この中央コンピュータ装置が適当な送信チャンネルを用いてデジタルメッセージをテレビ視聴者の個々の電子参加機械に放送し、且つ、時間カウント手段を初期化して作動させ、聴衆がそれ以上シナリオに参加できなくなる時間として選択された所定の時間Ｔ３に、時間カウント値を記憶して、このカウントを継続し、電子参加機械が中央コンピュータに接続される時間として選択された時間Ｔ５に、電子参加機械によって得られた時間カウント値を記憶し、以下の関係をチェックする：

【００２２】Ｔｒ２５＞Ｔａ３５およびＴｒ１２＋Ｔｒ２５＝Ｔａ１５±許容範囲値

ここで：Ｔｒ２５はＴ２とＴ５の間の電子参加機械によるカウント期間であり、Ｔｒ１２はＴ１とＴ２の間の電子参加機械によるカウント期間であり、Ｔｒ３５はＴ３とＴ５の間の中央コンピュータによるカウント期間であり、Ｔｒ１５はＴ１とＴ５の間の中央コンピュータによるカウント期間である。

【００２３】各ゲーム機械（電子参加機械）には、マイクロ回路カード用の安全保護されたマイクロプロセッサが備えられている。もう１つの具体例によれば、このマイクロ回路は、商業的に入手可能な種類のカード読み取り装置として機能する機械に挿入される銀行のカードのような形態を有するカードに入っていてもよい。あるいは、安全保護された回路は、カード以外の携帯用の物品、例えばプラスチックの鍵またはその他任意の適当と思われる物品に内蔵されていてもよい。

【００２４】安全保護された回路はさらに、取外し可能とする必要がないと思われる場合には、上述したように、機械の主回路構成要素に直接据え付けることもできる。「安全保護されたマイクロプロセッサ」という言葉は、例えば現在銀行が配布している銀行カードのようなスマートカードの使用に利用されている、任意の保護がかけられているマイクロプロセッサを示すものと理解されたい。添付した図を参照して行う以下の記載により、本発明のその他の利点が明らかとなろう。以下の記載は単に例示のためのもので、本発明を限定するものではない。

【００２５】

【実施例】図４の図は、本明細書の末尾の表１に示された以下に述べるシーケンスの計測動作を可能にする、ゲームへの参加における安全保護されたシステムを示している。このシステムは、テレビ番組トランスミッタ10と、そのトランスミッタ10に結合されて、例えば上記の特許出願に記載のような暗号化された形態でゲームメッセージを送信することが可能な中央コンピュータユニット20とを備えたトランスミッタ／中央コンピュータ１を有する。

【００２６】トランスミッタ／中央コンピュータは、伝送手段30を介して、ユーザ宅に配置された受信機に接続されている。放送されるゲームに参加を希望するユーザは、受信機上でのコード化されたメッセージを読み取り、標準的な方法での中央コンピュータに接続することができるゲーム機械Ｌ１～Ｌｎを所有している。メッセージが送信される時間Ｔ１には、つまり、テレビ視聴者が質問される時には、送信センタとゲーム中央コンピュータ１は、ゲーム機械Ｌ１～Ｌｎに、例えば公知のカード操作用の秘密キーで署名した暗号のメッセージを送る。

【００２７】このメッセージの発信は、放映される信号と同じチャンネル内（例えばリターンフレーム内）か、

あるいは同じ媒体内の独立したチャンネル（例えば複数のテレビジョンチャンネルを伝達するケーブル上の、専用のＨＦチャンネル）か、あるいは異なる媒体のチャンネル（例えば、アメリカ合衆国のインタラクティブゲームネットワークスのようにＦＭラジオのチャンネル）に設けた専用のデータチャンネルである、送信チャンネル30によって行うことができる。

【００２８】データチャンネルは、信号のトランスミッタおよびサービス提供者からテレビ視聴者への一方向性のものである必要はない。ゲーム機械Ｌ１は、コードの形でテレビ受像機40のスクリーン41上に現れるこの信号を受信すると、これを、ゲーム機械内、あるいは以下に説明するように取外し可能な媒体に設置された、安全保護された構成要素ＣＳに送る。ゲーム機械は、例えば上記の特許に記載のようなタイプの公知の電子回路構成要素を備え、それによってゲーム機械は、テレビのスクリーンに現れるメッセージを受けて、回答メッセージを中央コンピュータへと送ることができる。

【００２９】安全保護された構成要素ＣＳは、図５に示されており、揮発性および不揮発性メモリ、つまり、ＲＡＭ作業メモリ110 、ＲＯＭプログラムメモリ120 およびＥＥＰＲＯＭデータメモリ130 を備えたマイクロプロセッサ100 を有する。構成要素ＣＳは、ゲーム機械のクロック信号発生器150 からのクロックパルスを受け、さらにブロック140 によって表した、ゲーム機械への接続手段を有する。メッセージがスクリーン上に現れると、マイクロプロセッサ100 が、このメッセージを受けて、通常の方法でその真偽を検証し、クロックパルスに基づく時間カウントサブプログラムの実行を開始させる。このサブプログラムは、ＲＯＭメモリ120に含まれている。

【００３０】実際、安全保護されたマイクロプロセッサが、絶対時間でなく、マイクロプロセッサに供給されるクロック周波数150 に比例する時間ユニットをカウントする。なぜなら、マイクロプロセッサは、このクロック信号以外の時間的基準を全く持たないからである。さらに、安全保護されたマイクロプロセッサ100 が、その不揮発性メモリＥＥＰＲＯＭ130 に、カウント動作を開始させた、暗号メッセージ（またはこのメッセージの影）を記録する。

【００３１】以下のことをより明確に理解するために、本明細書の末尾の表１を参照されたい。時間Ｔ２で、テレビ視聴者が、彼のゲーム機械Ｌ１を使って質問に回答すると、この回答が安全保護されたマイクロプロセッサ100 へ送られ、マイクロプロセッサ100 が、それを公知の揮発性メモリ130 に記録し、さらに、ユーザの回答を受け取った時点で到達していた時間カウント値を記録する。このイベントの直後に、安全保護されたマイクロプロセッサ100 はカウントを継続する。Ｔ３はテレビ視聴者が質問に回答することのできる絶対的な期限であることはかわらない。この時間には、ゲーム機械には特別何も起こらない。つまり、情報を受信せず、安全保護されたマイクロプロセッサは時間のカウントを継続する。

【００３２】時間Ｔ３で、中央処理ユニット21およびメモリ22（そのうちの１つにはカウントプログラムがロードされている）を含む標準的な処理手段20を備えた中央コンピュータ自身も、時間カウント動作を開始する。中央コンピュータは、中心であって、基準として使用されるので、このカウントを以下「絶対」カウントと呼ぶ。採用されるカウントは、非常に安定で、可能な限り実時間に近い近似を表しているものとする。Ｔ４は、質問に対する解答が、テレビ視聴者のスクリーン上に与えられる絶対的な時間である。この時間には特に何も起こらない。

【００３３】ゲームに参加した個々のテレビ視聴者からの特定のデータ要素の転送は、時間Ｔ４以降、例えばゲームの数時間後に、ゲーム機械40～40ｎを中央コンピュータ１に接続することによって行われる。多くのテレビ視聴者が参加していることもあるので、接続はおそらく、夜間行われるようにプログラムされる。テレビ視聴者のゲーム機械は、先に述べたデータチャンネルを放送するのに使用されたものと方向が反対である「リターンチャンネル」を介して、中央コンピュータに接続される。このリターンチャンネルは、テレビが双方向ケーブルによって放送されているならば、分配ケーブル上に直接形成してもよい。リターンチャンネルは、簡単なモデムにより、スイッチされた電話ネットワーク上に設定することもできる。その他可能なリターンチャンネルの使用が考えられる。図４における参照番号30は、装備されることの可能な１つまたは複数の送信チャンネルを表している。

【００３４】中央コンピュータ１とテレビ視聴者のゲーム機械Ｌ１（Ｌｎ）との間に、上記のいずれかの手段によって接続がなされると、次いで安全保護されたマイクロプロセッサ100 が、標準的な正当性証明作業を開始し、中央コンピュータの正当性を証明し、中央コンピュータによりそれ自身の正当性を証明する。この正当性証明の機構は、本発明の目的を全く変えることなく、秘密キーまたは公知のパブリックキーを用いた暗号システムに基づくものとすることができる。接続中に、安全保護されたマイクロプロセッサ100 が、中央コンピュータに、テレビ視聴者によって与えられ時間Ｔ２で記録された回答の値を送る。

【００３５】本発明では、マイクロプロセッサ100 はさらに、Ｔｒ１２とＴｒ２５の値を中央コンピュータに送る。ここで、Ｔｒ１２は、Ｔ１とＴ２の間に、安全保護されたマイクロプロセッサによって、テレビ視聴者のゲーム機械の中で計算された、相対的な現地時間であり（図３に示されているように）。Ｔｒ２５は、（図３に示されているような）Ｔ２とＴ５の間に、同じ安全保護

されたマイクロプロセッサによって計算された、相対的な現地時間である。テレビ視聴者の回答およびゲーム機械Ｌ１がその場で計算した時間の値は、その完全性を保証するために、暗号を用いたチェックサムと共に送信され、場合によっては、機密上の理由から、公知の任意な暗号化アルゴリズムによって暗号化することもできる。このことは、本発明の原則には全く影響しない。

【００３６】ここで、Ｔａ１５が、（図３に示すような）Ｔ１とＴ５の間に中央コンピュータによって計算された「絶対」時間を示し、Ｔａ３５が、（図３に示すような）Ｔ３とＴ５の間に中央コンピュータによって計算された「絶対」時間を示すものとする。本発明によるならば、中央コンピュータはその場合、最初にＴｒ２５＞Ｔａ３５であることを確認し、そして、Ｔｒ１２＋Ｔｒ２５＝Ｔａ１５±許容範囲値（許容範囲値はあらかじめ設定されている）であることを確認する。これらの関係が検証されれば、回答が受け入れられる。そうでない場合には、中央コンピュータがこれを拒絶する。

【００３７】つまり、もし詐欺行為を行おうとする個人が、実際はＴ３以降に回答したにもかかわらず、あたかもＴ３以前に回答したようにみせかけようとするならば、彼はＴｒ２５の値を人為的に増加させるためには、Ｔ２とＴ５の間にカードに与えられるクロック150 の周波数を上げねばならない。しかし、Ｔｒ１２＋Ｔｒ２５の合計がＴａ１５±許容範囲値に等しくならなくなるために、この操作は発覚してしまう。

【００３８】実行は困難であるが依然として可能である唯一の不正行為は、Ｔ１とＴ２の間に、安全保護されたマイクロプロセッサに与えられるクロック信号の周波数を、Ｔｒ１２＋Ｔｒ２５の合計がその法定値を保つために、Ｔ２とＴ５の間にそのクロック信号の周波数を上げねばならない量と正確に等しい分だけ下げるというものであろう。これを不可能にするためには、時間Ｔ３が時間Ｔ１に対して可変であることを確認するだけでよい（つまり、質問に回答するために視聴者に許される時間が質問ごとに異なるようにすればよい）。従って、詐欺行為を行おうとする個人は、続いてＴ２とＴ５の間にそのクロック信号の周波数を上げねばならない値が判らないために、Ｔ１とＴ２の間にクロック信号の周波数を下げることができる値を予知することができない。

【００３９】本発明により、スマートカード用として標準的な方法で使用され、特にそれ自体が安全保護されている正確な基準クロック信号を持たない、安全保護されたマイクロプロセッサにより、イベントＴ１、Ｔ２、Ｔ３およびＴ５の正確な時系列を保証することも可能である。

【００４０】図６は、本発明における特定の実施例を示すもので、安全保護された構成要素は、メモリカードＣの集積回路チップの形態をとる。つまりこの機械は、スクリーン上に表示されたメッセージを読み取ってテレビ視聴者の応答を入力するために、中央コンピュータとの接続に使用される部位Ｌ１と、取外し可能な部位、つまり、マイクロプロセッサを備えたメモリカードとを有する。部位Ｌ１には、このため、Ｌ１がカードを受け取れるようにするためのスロットＦと、カードのコネクタＣと適合して、Ｌ１がメモリカード読み取り機として機能することを可能にする（図示されていない）コネクタとがある。この実施例をもってすれば、本発明は特に、テレビジョン信号のスクランブル解除に対するセキュリティを確保するためにすでにスマートカードを使用している加入者テレビジョンシステムに適用されることができる。

【００４１】

【表１】

13　　14

トランスミッタ／ゲーム中央コンピュータ		ゲーム機械／受信機		テレビ視聴者／参加者
ゲームメッセージ	→	メッセージ受信 （時間Ｔ１） クロックパルスのカウント、 メッセージの記憶		
		回答の受信および記憶 カウント値の記憶	←	回答 （時間Ｔ２）
回答期限（Ｔ３）				
正解	→	正解の受信		
計算 Ｔａ１５とＴａ３５ 回答の受信および Ｔｒ１２とＴｒ２５ チェック Ｔｒ２５＞Ｔａ３５ Ｔｒ１２＋Ｔｒ２５＝ Ｔａ１５±許容範囲値	←	中央コンピュータとの 接続設定 記憶されていた回答の送信 Ｔｒ１２とＴｒ２５の送信		

【図面の簡単な説明】

【図１】　ゲームのイベントの時系列を示すタイミング図である。

【図２】　従来の技術によるカウントシーケンスを示す、図１と同様のタイミング図である。

【図３】　本発明のカウントシーケンスを示す、図１と同様のタイミング図である。

【図４】　ゲームシステムの原理を示した図である。

【図５】　本発明による、安全システムの詳細な図である。

【図６】　特定の実施例における機械の図である。

【符号の説明】

１・・・ゲーム中央コンピュータ

10・・・トランスミッタ

20・・・中央コンピュータユニット

＊21、ＣＰＵ・・・中央処理ユニット

22・・・メモリ

30・・・送信チャンネル

40、40n・・・テレビ受像機

41・・・スクリーン

100・・・マイクロプロセッサ

110・・・ＲＡＭ作業メモリ

120・・・ＲＯＭプログラムメモリ

130・・・ＥＥＰＲＯＭデータメモリ

140・・・接続手段

150・・・クロック信号発生器

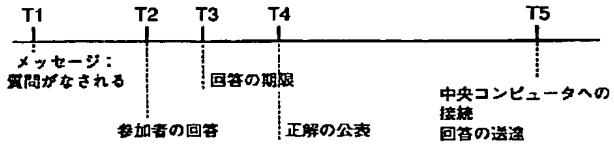
ＣＳ・・・安全保護された構成要素

Ｃ・・・メモリカード

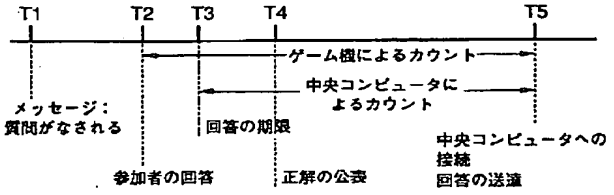
Ｆ・・・スロット

＊　Ｌ１、Ｌｎ・・・ゲーム機械

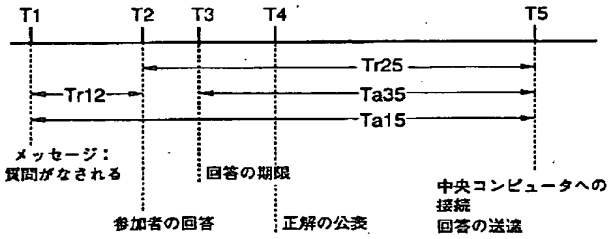
【図１】



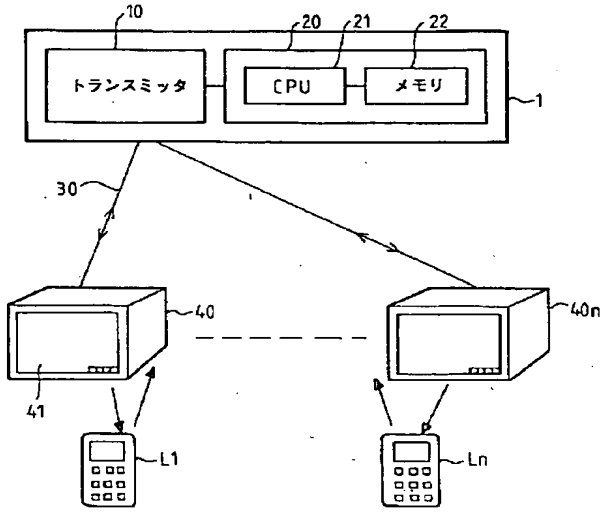
【図２】


T1
T2
T3
T4
T5
ゲーム機によるカウント
中央コンピュータによるカウント
メッセージ：質問がなされる
回答の期限
参加者の回答
正解の公表
中央コンピュータへの接続
回答の送達

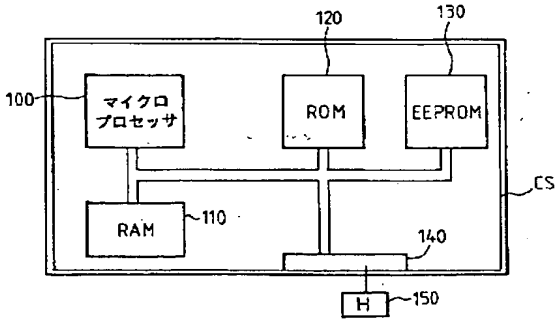
【図３】


T1
T2
T3
T4
T5
Tr25
Tr12
Ta35
Ta15
メッセージ：質問がなされる
回答の期限
参加者の回答
正解の公表
中央コンピュータへの接続
回答の送達

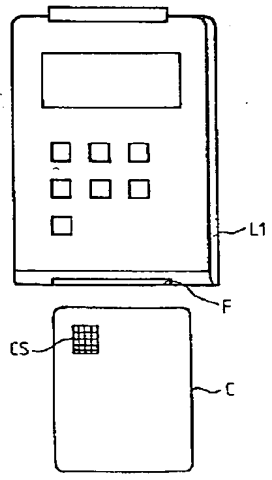
【図４】


10
20
21
22
トランスミッタ
CPU
メモリ
1
30
40
40n
41
L1
Ln

【図５】


120
130
100
マイクロプロセッサ
ROM
EEPROM
CS
RAM
110
140
H
150

【図６】


L1
F
CS
C

Bibliography

---

(19) [Country of Issue] Japan Patent Office (JP)
(12) [Official Gazette Type] Open patent official report (A)
(11) [Publication No.] JP,7-68051,A
(43) [Date of Publication] March 14, Heisei 7 (1995)
(54) [Title of the Invention] The safety system in the remote participation to an interactive game which verifies the time series of an event
(51) [International Patent Classification (6th Edition)]
A63F 9/22 G
H
G04F 10/04 9008-2F
[Request for Examination] Un-asking.
[The number of claims] 6
[Mode of Application] FD
[Number of Pages] 9
(21) [Filing Number] Japanese Patent Application No. 6-204521
(22) [Filing Date] August 5, Heisei 6 (1994)
(31) [Priority Document Number] 9309679
(32) [Priority Date] August 5, 1993
(33) [Country Declaring Priority] France (FR)
(71) [Applicant]
[Identification Number] 591032013
[Name] JIEMUPURYUSU Card ANTERU National SOSHIETE ANONIMU
[Name (in original language)] GEMPLUS CARD INTERNATIONAL SOCIETE ANONYME
[Address] France country 13420 JIEMUNO PARUKU DAKUTIVITE DOU RA PURENU DOU JUKU AVUNYU DOYU Pick DOUBERUTANYU (with no address)
(72) [Inventor(s)]
[Name] PATOLIS PEIRE
[Address] France country Schumann DOU Sun Francis RUKURO DOYU Methamphetamine (with no address)
(74) [Attorney]

[Patent Attorney]
[Name] **** **

[Translation done.]

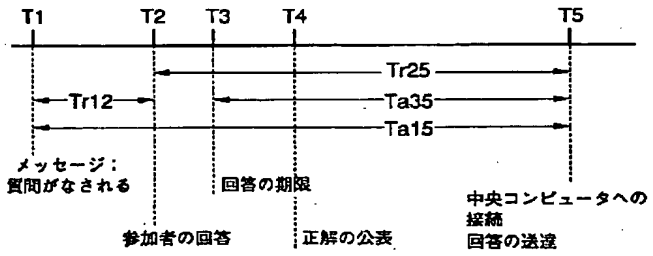
* NOTICES *

Summary

---

(57) [Abstract]
[Elements of the Invention] The safety system in the remote participation to an interactive game which verifies the time series of an event by the count of a continuous period using the secured microprocessor (for example, microcircuit card). Among those, the first period (Tr12) is started by the message secured using the code transmitted by the transmitter, and the last period (Tr25) is ended by the connection with the central computer of a transmitter for sending a reply to the central computer of a transmitter from a game machine.
[Function] It is used for the interactive game by which television televising is carried out.

[Translation done.]



[Translation done.]

* NOTICES *

CLAIMS

[Claim(s)]
[Claim 1] The safety system equipped with the transmitter / central computer which is characterized by providing the following and which transmits the code message received by the television set while a TV program is going on in the remote participation to an interactive game A TV viewer reads the broadcast message, has the possible game machine of returning the reply to the question made in these messages, and sets to this system. It has a means by which a game machine counts a continuous period. among these, the first period (Tr12) The message transmitted by the transmitter / central computer begins. the last period (Tr25) The connection with a transmitter / central computer from a game machine is completed. the first period It is specified by time (t2) for the time (t1) when a message is received, and a TV viewer to answer. the last period (Tr25) It is specified by time (t2) for a TV viewer to answer and the time (t5) when a reply is sent to a transmitter / central computer. further a game machine The period when it has a means for transmitting a reply to a transmitter / central computer with the above-mentioned count result in, and a transmitter / central computer is specified by the term (t3) of a reply, and the time (t5) when the reply was sent (ta35) A means to count the period (ta15) specified by the time (t1) when the message was transmitted, and the time (t5) when the reply has been sent Tr25>Ta35 And the calculation and the check means which are constituted so that a reply may be refused, when a relation called the value of Tr12+Tr25=Ta15** tolerance is checked and this relation is not verified further
[Claim 2] The safety system in the remote participation to the interactive game according to claim 1 characterized by the count means of a game machine being constituted by the secured microprocessor which performs a clock pulse count program, and which is controlled by the clock.
[Claim 3] The safety system in the remote participation to the interactive game according to claim 1 characterized by the count means of a game machine being constituted by calculation means controlled by the internal clock to perform a clock pulse count program.
[Claim 4] The machine for participating in a program and attesting participation in

cooperation with a remote central computer characterized by providing the following The means for receiving the digital information sent from a central computer The interface means for a participant introducing the data element showing a participant's participation The means for connecting with a central computer A microprocessor and its storage means

[Claim 5] The machine for participating in the program according to claim 4 characterized by having had the chip card reading means and the chip card, and equipping the above-mentioned chip card with the component from which the form of the integrated-circuit chip card which has a microprocessor, work memory, and program memory was secured.

[Claim 6] It is the central computer apparatus which manages the participation to the broadcast scenario of the TV viewer who has an electronic participating machine. A time count means, A means to broadcast a digital message to each electronic participating machine, and the means for making connection with each electronic participating machine, If it has the storage processing means and a new broadcast scenario is started This central computer apparatus uses a suitable transmitting channel for time T1, and broadcasts a digital message to each electronic participating machine of a TV viewer at it. Furthermore, initialize a time count means, operate it and a TV viewer memorizes time counted value at the predetermined time T3 chosen as time it becomes impossible to participate in a scenario more than it. this -- a count -- continuing -- an electron -- participation -- a machine -- a center -- a computer -- connecting -- having -- time -- ****** -- choosing -- having had -- time -- T -- five -- an electron -- participation -- a machine -- obtaining -- having had -- time -- counted value -- memorizing -- the following -- a relation -- checking -- : -- Tr -- 25 -- > -- Ta -- 35 -- :Tr25 is a count period by the electronic participating machine between T2 and T5 here. a Tr12+Tr25=Ta15** tolerance value -- Tr12 is equipment which is a count period by the electronic participating machine between T1 and T2, and Tr35 is a count period by the central computer between T3 and T5, and is characterized by Tr15 being a count period by the central computer between T1 and T5.

[Translation done.]

* NOTICES *

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Industrial Application] this invention relates to the unjust prevention system or safety system in remoteness or long-distance participation to an interactive game which verifies the time series of an event.
[0002]
[Description of the Prior Art] With the advent of the so-called interactive-mode television system, to enable participation to a televiewer's game which is called for so that a televiewer may answer to the question broadcast from the office is desired for example, during broadcast. In order to prevent a TV viewer's answering after the correct answer of a game is shown from an office, or answering in the midst of such a game after referring to a various-subjects dictionary and reference databases arbitrary in addition to this, the maximum reply time must be set up. Furthermore, in order that the feeders (a cable operator, broadcast studio, etc.) of service may avoid "being saturated" by the reply of thousands sent simultaneously, as for a reply of a TV viewer, it is desirable to make it not sent immediately. For that purpose, an accumulation transmitting system is indispensable. In this system, it is a safe method, and a reply of a TV viewer is memorized by the devices for the public (for example, a cable decoder, the game machine of exclusive use, etc.), and behind, it is the televiewer's home and it is sent [it shifts time suitably and] by the suitable telecommunication means of a radiotelephone and other arbitration [a cable and].
[0003] There are some which were developed for example, developed by the interactive game networks (Interactive Game Networks) company as an example of such a system in the United States of America. In this system, a TV viewer has the small game machine with which a radio interface, the keyboard, the screen, the modem, and the security module were formed. In order to understand operation of such a system, please refer to drawing 1 which showed the time series of an event.
[0004] In time T1, a question is broadcast from the transmitter / central computer called a "central computer" below. These questions are broadcast with radio to the above-mentioned game machine. For example, at the time of the start of a game of football, a TV viewer is called for so that the score of the first half may be expected. This question appears on the screen of a game machine. A reply is inputted through the key boat of a game machine by each TV viewer who has participated in time T2, and it is recorded on the safe chip (thing of the type currently used by the smart card) with which the game machine is equipped. A new broadcast signal locks all game machines, and it is made not to receive any replies any more after [of since a question is performed] several minutes at time T3. Then, the answer to a question is broadcast in time T4 (in this example, T4 is actually equivalent to halftime). Then, the reply recorded on time T5 is sent to the central computer of a game through an

exchange formula telephone network by the modem, and serves as proof of participation. If a TV viewer answers correctly, he/she will receive a certain prize or prize.

[0005] American ****** According to a practice like [of No. 4,592,546] a publication, the date (time) of each event is recorded using the clock circuit which has sufficient precision installed in the game machine. When a reply of a participant is sent to the central computer of a game, the time recorded with the game machine is also sent to a central computer, and it is compared with the conventional time saved in it by the computer.

[0006] According to the practice otherwise proposed, in each public type game machine, the reference clock signal transmitted from the central computer of a game and the electronic real time clock circuit synchronized for every fixed interval (for example, radio combination) possess. The time T1 when a question is broadcast, and the time T2 when a reply is made are recorded on a game machine (for example, recorded in the chip for smart cards by the secured method). If connection is made to a game central computer, the time recorded as the reply will be spent as a proof of participation. A central computer is within the limits which can permit the information concerning an air time T1, and checks that T2 is a front [3 / T/ which is reply term].

[0007]

[Problem(s) to be Solved by the Invention] In addition to this in the above-mentioned system, the user who had malice in the analogous embodiment may record the control signals (a question, a locking instruction, clock synchronization-ized signal, etc.) sent to his game machine on a suitable machine.

[0008] In this case, if the place which the answer to a question is broadcast from an office, or he knows by a special search or arbitrary meanses in addition to this comes when slightly behind, the individual with this malice can repeat a control signal in his own game machine, and can pretend the reply of real time. This becomes possible for the time of length appropriate always enough passing before attainment of the reply to the central computer which a witness does not break into the individual who performs a fraud action in the privacy of a house, but is further expected to a degree from a play end. It is economically impossible to equip a game machine with the means for knowing whether it is what slight delay is given, after the real time occurs truly or the signal (this should be made safely) which it received from the outside is recorded completely without correction in them on a game machine after all.

[0009] the France patent application 89th -- it applies as No. 06848 -- having -- the France patent application public presentation official report 2nd -- the patent exhibited as 647 619 No. -- and -- coming out -- the France patent application public presentation ****** the France addition patent 90th exhibited as 2 658 357 No. -- delaying a play to No. 01512 -- the system which enables unjust prevention is indicated The time T3 when the answer was broadcast for the central computer in

the system (or reply term), The reply by the TV viewer counts the absolute time which passes between the time T5 sent to the central computer, and sets at time T2. By reply of a TV viewer, local time count operation within a game machine is started. Time T5–T2 by which this central computer is measured with the game machine of ******** at the time T5 when information is sent to a central computer check that it is size more nearly rightly than absolute–time T5–T3 which itself calculated.

[0010] The timing chart shown in drawing 2 shows the above sequence. The method proposed by this patent is not trustworthy by any means to a regrettable thing. A user is because it can show between a reply and connection with a central computer as if time T5–T2 [longer than the time which actually passed] passed by advancing a local time counter. This becomes possible only by correcting temporarily the oscillation frequency of the electronic clock circuit placed into the game machine.

[0011] Actually, the counter in a game machine is accessible for a user, unless it is protected physically (i.e., unless it is embedded in the resin). Even if this circuit is supplied by any of an RC oscillator, ceramic resonator type VCO, or a crystal oscillator, the original frequency can be distorted by few [an oscillating element] mismatches. Therefore, it is possible to make oscillation frequency high by few percentages, or to make it late, without being accompanied by exceptional difficulty. By making high oscillation frequency of the VCO supplied to the clock circuit of a game machine, oscillation frequency of the VCO of a game machine is made high waiting (it is waiting about an answer being broadcast live), and after that, and they can regain delay until a term T3 passes over those who are going to perform a fraud action. Therefore, when this individual's game machine receives an inquiry from a central computer in time T5, time T5–T2 of the appearance given to this central computer become long actually more rather.

[0012] The method of equipping the microprocessor of a microcircuit card of a certain kind with the clock frequency detector for detecting the abnormalities of a clock frequency is learned. In order for the individual whom this kind of detector tends to give for example, a fraud action to prevent trying the "step–by–step" method to the program by which a processor performs, the clock frequency supplied to this component operates extremely at the time of a low. such [typically] a low frequency detector –– the nominal frequency of the component –– 1MHz – 5MHz it is –– sometimes, it operates by less than about 500kHz Serious lack of the precision in this kind of detector and the fact of existing only in order that it may detect low frequency extremely mean that it cannot use it in order to prevent injustice above type.

[0013] this invention aims at conquering the fault of the system used now. Actually, the system set as the object of this invention can be used, in order that a TV viewer may verify certainly rightly the fact of having replied to the question between the terms determined by the transmitting person of time and a game to whom the question was performed.

[0014]
[Means for Solving the Problem] The message secured using the code in which the first interval is transmitted by the transmitter begins [the system proposed here counting the time interval which continues by the secured processor (for example, microcircuit card processor)], and the last interval is ended by making connection with a central computer from a game machine, in order to send the proof of a reply to a central computer.
[0015] More, a detail will be provided with the safety system equipped with the transmitter / central computer which transmits the code message received by the television set during advance of a TV program in the remote participation to an interactive game, if based on this invention. A TV viewer reads the broadcast message and it has the possible game machine of returning the reply to the question made in these messages. The length Tr12 of the period specified by the time t2 for the time t1 when a message is received for a game machine, and a TV viewer to answer in this system, It has a means to count the length Tr25 of the period specified in the time t2 for a TV viewer to answer and time t5 when a reply is sent to a transmitter / central computer, and is [0016]. The length ta35 of the period when a transmitter / central computer is specified by the term t3 of a reply, and the time t5 when the reply was sent, It has a means to count the length ta15 of the period specified by the time t1 when the message was transmitted, and the time t5 when the reply has been sent. Furthermore, a relation called the value of Tr25>Ta35 and Tr12+Tr25=Ta15** tolerance was checked, and when this relation is not verified further, it has a calculation means to refuse a reply. The count means of a game machine is constituted by the secured microprocessor which performs a clock pulse count program and which was controlled by the clock.
[0017] The machine for according to this invention, participating in a program and attesting participation in cooperation with a remote central computer further By means to receive the digital information sent from a central computer, and the participant The interface for introducing the data element showing a participant's participation, It has the means for connecting with a central computer, a microprocessor and at least one secured electronic component equipped with the storage means, and at least one clock signal generating circuit, and is [0018]. If a machine receives the digital message which has a form predetermined in time T1 Send to the microprocessor which had the message secured, and the microprocessor secured after verification records this message on the memory. The count of a time [to be proportional to the period of the clock signal given by the clock signal generating circuit] unit is started. in time T2 When a machine receives the data element about his participation from the TV viewer who owns this machine, a machine The data element is transmitted to the secured microprocessor, this microprocessor records the data into the memory with a required form, and records this instantaneous time counted value further, and it is [0019]. A reply can be refused, when a microprocessor transmits the data element and counted value Tr12

and Tr25 about the memorized participation, a central computer verifies that these values are in agreement with the counted value of itself and it is not further in agreement, shortly after the secured microprocessor continues a count and connection is made in time T5 until the machine is connected with a central computer by means to connect.

[0020] Furthermore, the central computer apparatus which manages the participation to the broadcast scenario of the TV viewer who has an electronic participating machine according to this invention is equipped with the time count means, a means to broadcast a digital message to each electronic participating machine, the means for making connection with each electronic participating machine, and the storage processing means, and is [0021]. If a broadcast scenario is started, this central computer apparatus will use a suitable transmitting channel for time T1, and will broadcast a digital message to each electronic participating machine of a TV viewer at it. And initialize a time count means, operate it and an audience memorizes time counted value at the predetermined time T3 chosen as time it becomes impossible to participate in a scenario more than it. : which continues this count, memorizes the time counted value obtained by the electronic participating machine at the time T5 chosen as time when an electronic participating machine is connected to a central computer, and checks the following relations

[0022] Tr25>Ta35 and a Tr12+Tr25=Ta15** tolerance value -- Tr12 is a count period by the electronic participating machine between T1 and T2, :Tr25 is a count period by the electronic participating machine between T2 and T5 here, and Tr15 is [Tr35 is a count period by the central computer between T3 and T5, and] a count period by the central computer between T1 and T5

[0023] Each game machine (electronic participating machine) is equipped with the microprocessor from which it secured for microcircuit cards. According to another example, this microcircuit may be contained in the card which has a gestalt like the card of a bank inserted in the machine which functions as a card reader of an available kind commercially. Or in addition to this, the secured circuit may be built in portable goods other than a card, for example, the key of plastics, and the arbitrary goods considered to be suitable.

[0024] When it is thought that the secured circuit does not need to make removal still more possible, as mentioned above, it can also install directly to the main circuit component of a machine. Please understand the word "secured microprocessor" to be what shows the microprocessor which is used for use of a smart card like the bank card which for example, the present bank has distributed, and to which arbitrary protection is applied. By the following publications performed with reference to appended drawing, the advantage of others of this invention will become clear. The following publications are the things for instantiation only, and do not limit this invention.

[0025]

[Example] Drawing of drawing 4 shows the secured system in the participation to a

game which enables measurement operation of the sequence stated to the following shown in Table 1 of the tail of this specification. This system has a transmitter / central computer 1 equipped with the central computer unit 20 which it is combined with the TV program transmitter 10 and its transmitter 10, for example, can transmit a game message to the above-mentioned patent application with an enciphered gestalt like a publication.

[0026] The transmitter / central computer is connected to the receiver arranged at user ** through the transmission means 30. The user who expects participation of the game broadcast reads the coded message on a receiver, and owns the game machines L1-Ln connectable with the central computer in a standard method. When it is got blocked and a TV viewer is asked, a transmitting center and the game central computer 1 send the message of a code which signed game machines L1-Ln, for example by the well-known secret key for card operation at the time T1 when a message is transmitted.

[0027] The transmitting channel 30 which is a DCH of the exclusive use prepared in the channel (a channel of FM radio like [For example,] U.S.'s interactive game networks) of the inside of the same channel as the signal broadcast (for example, inside of a return frame), the channel (for example, HF channel of exclusive use on the cable which transmits two or more television channels) which it became independent of in the same medium, or a different medium can perform dispatch of this message.

[0028] A DCH does not need to be the thing of one directivity from the transmitter and service provider of a signal to a TV viewer. A game machine L1 will be sent to the secured component CS which was installed in the medium which can be removed so that this might be explained to the following in a game machine, if this signal that appears on the screen 41 of a television set 40 in the form of a code is received. A game machine can equip the above-mentioned patent with the well-known type electronic-circuitry component like a publication, and a game machine can send a reply message to a central computer in response to the message which appears in the screen of television by it.

[0029] It is shown in drawing 5 and the secured component CS is volatility and non-volatile memory 110, i.e., RAM work memory, and the ROM program memory 120. And EEPROM data memory 130 Microprocessor 100 which it had It has. Component CS -- clock signal generator 150 of a game machine from -- a clock pulse -- receiving -- further -- block 140 It has the connecting means to the game machine which expressed. It is a microprocessor 100 when a message appears on a screen. The truth is verified by the usual method and execution of the time count subprogram based on a clock pulse is made to start in response to this message. This subprogram is contained in the ROM memory 120.

[0030] Clock frequency 150 by which the secured microprocessor is actually supplied to the microprocessor instead of an absolute time A time [to be proportional] unit is counted. A microprocessor is because it does not have time

criteria other than this clock signal at all. Furthermore, secured microprocessor 100 The non-volatile memory EEPROM130 The code message (or shadow of this message) which made count operation start is recorded.

[0031] In order to understand the following things more clearly, please refer to Table 1 of the tail of this specification. Microprocessor 100 from which this reply was secured when the TV viewer replied to the question in time T2 using his game machine L1 It is sent and is a microprocessor 100. It is the well-known volatile memory 130 about it. It records and the time counted value which had reached further when the reply of a user was received is recorded. Microprocessor 100 secured just behind this event A count is continued. It does not change T3 that it is the absolute term which a TV viewer can answer to a question. Nothing happens to a game machine specially at this time. That is, information is not received but the secured microprocessor continues the count of time.

[0032] The central computer itself equipped with the standard processing means 20 containing the central-process unit 21 and memory 22 (the count program is loaded to one of them) in time T3 starts time count operation. A central computer is a center, and since it is used as criteria, it calls this count "absolute" count below. The count adopted shall be very stable and shall express approximation near the real time as much as possible. T4 is absolute time when the answer to a question is given on a TV viewer's screen. Nothing special happens at this time.

[0033] A transfer of the specific data element of each TV viewer who participated in the game is performed by connecting game machines 40-40n to the central computer 1 after time T4 (for example, several hours after a game). Since many TV viewers may have participated, probably connection is programmed to be carried out night. The thing and direction which were used for a TV viewer's game machine broadcasting the DCH described previously are connected to a central computer through opposite "return channel." If television is broadcast by the bidirectional cable, you may form this return channel directly on a distribution cable. A return channel can also be set up on the switched telephone network with an easy modem. In addition, use of a possible return channel can be considered. The reference number 30 in drawing 4 expresses one or more possible transmitting channels of being equipped.

[0034] Microprocessor 100 subsequently secured when connection was made by one of the above-mentioned meanses between the central computer 1 and a TV viewer's game machine L1 (Ln) Standard justification proof work is started, the justification of a central computer is proved, and the justification of itself is proved by central computer. The mechanism of this justification proof shall be based on the code system using the secret key or the well-known public key, without completely changing the purpose of this invention. Microprocessor 100 secured during connection The value of the reply which was given to the central computer by the TV viewer and was recorded on it in time T2 is sent.

[0035] At this invention, it is a microprocessor 100. The value of Tr12 and Tr25 is

further sent to a central computer. Here, Tr12 is the relative local time calculated in a TV viewer's game machine by the microprocessor secured between T1 and T2 (it is shown in drawing 3 like). Tr25 is the relative local time calculated by the secured same microprocessor between T (as [show / in drawing 3])2, and T5. It is transmitted with the checksum which used the code and the value of the time which the reply of a TV viewer and the game machine L1 calculated on that spot can also be enciphered by well-known arbitrary encryption algorithms from the reasons of secrecy depending on the case, in order to guarantee the integrity. This does not influence the principle of this invention at all.

[0036] Here, Ta15 shall show the "absolute" time calculated by central computer between T (as [show / in drawing 3])1, and T5, and Ta35 shall show the "absolute" time calculated by central computer between T (as / show / in drawing 3])3, and T5. If based on this invention, a central computer will check that it is Tr25>Ta35 first in that case, and it will check that it is a Tr12+Tr25=Ta15** tolerance value (the tolerance value is set up beforehand). A reply will be accepted if these relations are verified. When that is not right, a central computer refuses this.

[0037] That is, it is the clock 150 given to a card between T2 and T5 in order for him to make the value of Tr25 increase artificially, if the individual who is going to perform a fraud act is going to show as it answered before T3 although he answered in practice after T3. You have to raise frequency. However, since the sum total of Tr12+Tr25 stops becoming equal to a Ta15** tolerance value, this operation will be revealed.

[0038] Although execution is difficult, the still possible only malfeasance lowers only a part equal to the amount and accuracy which must raise the frequency of the clock signal between T2 and T5, in order that the sum total of Tr12+Tr25 may maintain the legal value for the frequency of the clock signal given to the microprocessor secured between T1 and T2. In order to make this impossible, time T3 should just check that it is adjustable to time T1 (what is necessary is just to make it, in order to get it blocked and to reply to a question (the time which a televiewer is allowed differ for every question)). Therefore, since the individual who is going to perform a fraud act does not understand the value which must raise the frequency of the clock signal between T2 and T5 continuously, he cannot foreknow the value which can lower the frequency of a clock signal between T1 and T2.

[0039] It is also possible to guarantee the exact time series of events T1, T2, T3, and T5 by the secured microprocessor which is used by the method standard as an object for smart cards by this invention, and does not have the exact reference clock signal with which especially itself is secured by it.

[0040] The component which drawing 6 shows the specific example in this invention, and was secured takes the form of the integrated circuit chip of memory card C. That is, in order that this machine may read the message displayed on the screen and may input a TV viewer's response, it has, the part L1 used for connection with a central computer, and the part which can be removed, i.e., the memory card

equipped with the microprocessor. For this reason, a part L1 is suited with the slot F for L1 receiving a card, and the connector C of a card, and there is a connector which enables L1 to function as a memory card reader (not shown) in it. If it carries out with this example, especially this invention is applicable to the subscriber television system which has already used the smart card, in order to secure the security to scramble release of a television signal.

[0041]

[Table 1]

トランスミッタ／ゲーム中央コンピュータ		ゲーム機械／受信機		テレビ視聴者／参加者
ゲームメッセージ	→	メッセージ受信 （時間Ｔ１） クロックパルスのカウント、 メッセージの記憶		
		回答の受信および記憶 カウント値の記憶	←	回答 （時間Ｔ２）
回答期限（Ｔ３）				
正解	→	正解の受信		
計算 Ｔａ１５とＴａ３５ 回答の受信および Ｔｒ１２とＴｒ２５ チェック Ｔｒ２５＞Ｔａ３５ Ｔｒ１２＋Ｔｒ２５＝ Ｔａ１５±許容範囲値	←	中央コンピュータとの 接続設定 記憶されていた回答の送信 Ｔｒ１２とＴｒ２５の送信		

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DESCRIPTION OF DRAWINGS

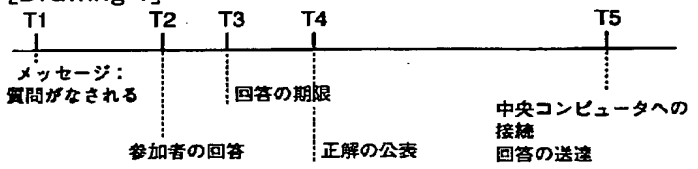
[Brief Description of the Drawings]
[Drawing 1] It is the timing chart showing the time series of the event of a game.
[Drawing 2] It is the same timing chart as drawing 1 showing the count sequence by the Prior art.
[Drawing 3] It is the same timing chart as drawing 1 showing the count sequence of this invention.
[Drawing 4] It is drawing having shown the principle of a game system.
[Drawing 5] It is detailed drawing of a safety system by this invention.
[Drawing 6] It is drawing of the machine in a specific example.
[Description of Notations]
1 ... Game central computer
10 ... Transmitter
20 ... Central computer unit
21 CPU ... Central-process unit
22 ... Memory
30 ... Transmitting channel
40 or 40n ... Television set
41 ... Screen
100 ... Microprocessor
110 ... RAM Work Memory
120 ... ROM Program Memory
130 ... EEPROM Data Memory
140 ... Connecting Means
150 ... Clock Signal Generator
CS ... Secured component
C ... Memory card
F ... Slot
L1, Ln ... Game machine

[Translation done.]

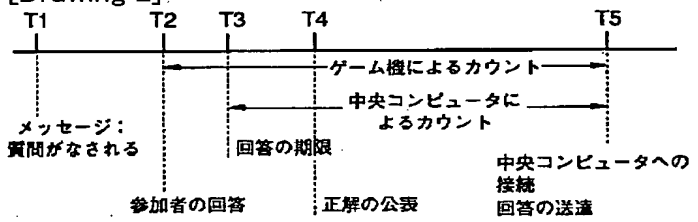
* NOTICES *

DRAWINGS

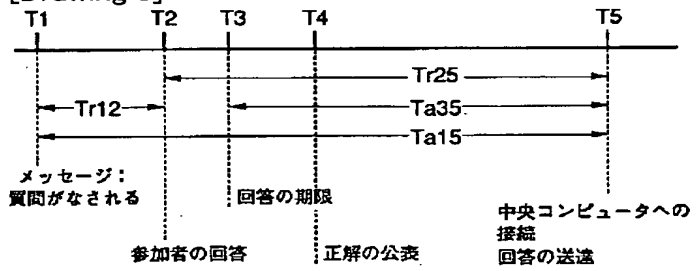
[Drawing 1]



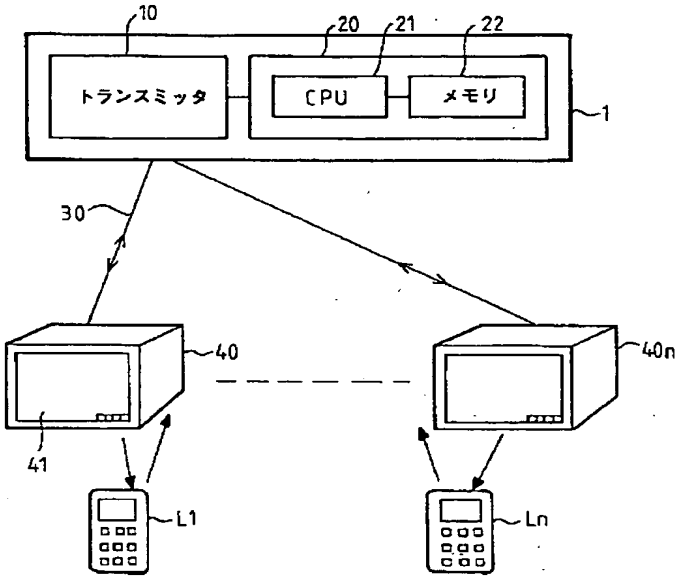
[Drawing 2]



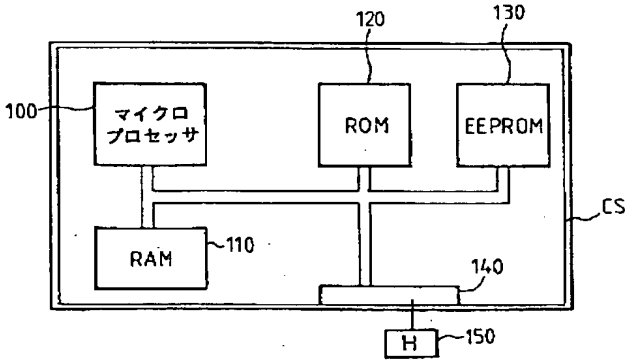
[Drawing 3]



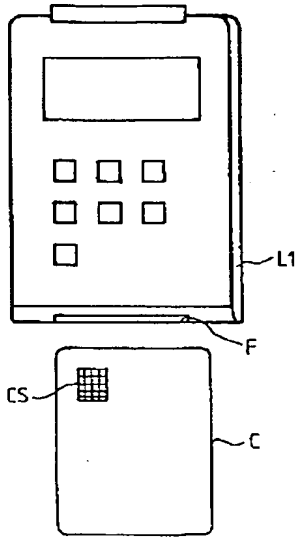
[Drawing 4]



[Drawing 5]



[Drawing 6]



[Translation done.]